UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 12/05/2012

Browdy and Neimark, PLLC
1625 K Street, N.W.
Suite 1100
Washington, DC 20006

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
12/05/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/771,967	AKKAR ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 November 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *15-19,23,24,27-34,36 and 37* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *15-19,23,24,27-34,36 and 37* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 02 November 2011 has been entered.

2. By the above submission, Claims 23, 27-29, 32, and 34 have been amended. Claim 22 has been canceled. New Claims 36 and 37 have been added. Claims 15-19, 23, 24, 27-34, 36, and 37 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 02 November 2011 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 15-19, 23, 24, 27-34 under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783, with general reference to independent

Claim 34 and new independent Claim 36, Applicant makes various characterizations of the prior art references (see pages 10-13 of the present response); however, Applicant's arguments do not clearly comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

More specifically, Applicant argues that Chow, individually, "fails to recognize that there may be any random selection" (pages 11-12 of the present response, citing Chow, column 18, line 50-column 19, line 13, *inter alia*). In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). It is noted that Kocher was relied upon for disclosure of choosing operations in a chain of operations depending on a random decision (Kocher, column 9, lines 1-13, as previously cited).

Applicant further argues that Chow deals with a different technical problem than that considered by the inventors (page 12 of the present response). In response to applicant's argument that Chow is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Chow is at

least reasonably pertinent to the particular problem with which Applicant was concerned; in particular, Chow is directed to tamper resistance techniques (Chow, title, abstract, and throughout). The claimed invention recites an intended use of resisting differential power attacks against a microcircuit card (see the preambles of Claims 34 and 36). Resisting various attacks is a type of tamper resistance, and therefore, since both the claimed invention and Chow are directed to tamper resistance, Chow is, at the very least, reasonably pertinent to the problem with which Applicant is concerned. See also MPEP §§ 2141 and 2141.01(a).

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (page 12 of the present response), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicant further argues that Kocher "fails to realize any possible use in case of validation" with a comparison of results as claimed (page 12 of the present response). Again, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

1986). The admitted prior art does disclose such a validation, and further discloses that DES can be used to perform such a validation (see page 2, lines 3-11, of the present specification). Kocher explicitly discloses modifications that can be made to DES (see title and abstract, and throughout), where Kocher more specifically discloses that operations in a chain of operations can be chosen depending on a random decision (see Kocher, column 9, lines 1-13, as previously cited). In combination with the teachings of using DES for validation, as admitted by Applicant, and determining whether to use an operation in its normal or complemented state, as taught by Chow, Kocher at least suggests performing the determination of whether to perform the operation or its complement in a random manner, in order to increase the security of a system using DES (see Kocher, column 1, line 66-column 2, line 9, as previously cited).

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Objections

4. The objection to Claim 34 for informalities

5. Claims 27, 28 are objected to because of the following informalities:

Claims 27 and 28 each recite “a one of the operations” in line 4 of each claim. It appears that “a one” should instead read “one”.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 15-19, 23, 24, and 27-34 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn because the amendments have raised new issues of indefiniteness, as detailed below.

7. The following is a quotation of 35 U.S.C. 112(b):

> (B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 15-19, 23, 24, 27-34, 36, and 37 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant, regards as the invention.

Claim 34 recites “said first chain of operations forming a data encryption method providing a Data Encryption Standard” in lines 6-7. It is not clear what is meant by the phrase that the method provides a data encryption standard. First, the use of the article “a” makes it unclear whether this is intended to refer to the specific algorithm known as DES, or if it is intended to refer to a general standard for encrypting data. Further, it is not clear how a method would provide a standard; it would appear that a method could be performed according to a standard but that a chain of operations could not in itself provide a standard, as claimed. The claim further recites “this message” in line 14, “this microcircuit card” in line 22; and “this key and this message” in line 29. The antecedent

basis of these limitations is not clear; in particular, it is not entirely clear if "this" is being used in a manner analogous to "the" or "said" or if a different meaning is intended. The claim also recites "sending this message to the server entity" in line 14. It is not clear from where this message is sent. Claim 34 further recites "using said key and said message when received" in line 16. It is not clear what the subject of the verb "received" is intended to be; that is, it is not clear whether only the message is received or if both the key and the message are received. The claim additionally recites the step of executing instructions in the microcircuit card with "this message" in lines 29-30. It is not clear whether the microcircuit card ever receives the claimed message, and therefore it is not clear how it would be able to use such message. All of the above renders the claim indefinite.

Claim 23 recites "which of said operations to choose" in line 3. There is not clear antecedent basis for this limitation in the claims, although it appears that this is intended to refer to the choosing one of the groups of operations recited in Claim 34, lines 20-23.

Claim 24 recites "computing a parameter which is equal to a difference between a number of times when an operation of the first chain of operations is executed and a number of times when an operation of the second chain of operations is executed" and that "the step of randomly choosing is conducted so as to decrease the difference". This is generally unclear, because Claim 34 recites choosing between performing either all of the operations of the first chain or all of the operations of a second chain. There only appears to be one step of randomly choosing, and it occurs before any of the operations are executed, so it is not clear how the step of randomly choosing can be

conducted to decrease the difference between the numbers of times operations are executed. Further, since all of the operations in one chain or the other are chosen and executed, it is not clear what calculating this difference parameter would accomplish.

Claim 31 recites "said third group" in lines 2-3 and "the random selection" in line 4. There is insufficient antecedent basis for these limitations in the claims. Further, because all of the subsequent limitations appear to depend on the "random selection", it has not been possible to clearly determine the scope of these steps.

Claim 32 recites "said third group" in lines 2-3 and "the random selection" in line 4. There is insufficient antecedent basis for these limitations in the claims. Further, because all of the subsequent limitations appear to depend on the "random selection", it has not been possible to clearly determine the scope of these steps.

Claim 33 recites "said third group" in lines 2-3 and 7. There is insufficient antecedent basis for this limitation in the claims. Further, because all of the claim limitations depend on this step of determining operations in a third group which does not clearly exist, it has not been possible to clearly determine the scope of these steps.

Claim 36 recites "said first chain of operations forming a data encryption method providing a Data Encryption Standard" in lines 6-7. It is not clear what is meant by the phrase that the method provides a data encryption standard. First, the use of the article "a" makes it unclear whether this is intended to refer to the specific algorithm known as DES, or if it is intended to refer to a general standard for encrypting data. Further, it is not clear how a method would provide a standard; it would appear that a method could be performed according to a standard but that a chain of operations could not in itself

provide a standard, as claimed. The claim further recites "the message coming from the server entity" in line 18; there is not clear antecedent basis for this limitation in the claims, although for purposes of interpreting the prior art it has been assumed that this is intended to refer to the message sent in line 13 of the claim. The claim also recites "said each operation or a respective operation in the second chain" in lines 20-21. This "respective operation" is not clearly defined in the claim. Claim 36 additionally recites "the successive random selections" in lines 26-27. There is insufficient antecedent basis for this limitation in the claim. All of the above renders the claim indefinite.

Claim 37 uses the pronoun "it" in line 2; care should be taken to ensure that the antecedents of pronouns are clear.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 15-19, 23, 24, 27-34, 36, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In reference to Claim 34, Applicant admits as prior art a method that includes storing a first chain of operations that performs DES encryption, sending a request from a server entity and a microcircuit card for generating a message and sending the message to the server entity, the server entity executing a first set of instructions applying a first chain of operations to the message to obtain a server result, the microcircuit card executing a second set of instructions applying a chain of operations to the message to obtain a resultant message, comparing the resultant message to the server result, and the server and card mutually authenticating when the server result and resultant message are identical (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly choosing a group of operations that include first and second chains of operations in either a complemented or uncomplemented state.

Chow discloses a tamper-proof encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the

tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9). However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53). Applicant also admits as prior art that operations are used in the DES algorithm, which by definition includes at least XOR and permutation operations (see page 1, line 21-page 2, line 11 of the present specification).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 23 and 32, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and intermediate responses are transmitted (see Kocher, column 2, lines 17-19), and Chow further discloses transmitting information with each executed operation (Chow, column 19, lines 22-34).

In reference to Claims 24 and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30; see also column 7, lines 21-29).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

In reference to Claim 31, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and a counter is updated (Kocher, column 9, lines 25-27; column 10, lines 13-column 11, line 26; column 11, lines 41-45).

In reference to Claim 36, Applicant admits as prior art a method including storing a first chain of operations that performs DES encryption, exchanging a message between a server entity and a microcircuit card, the server entity executing a first set of instructions applying the first chain of operations to the message to obtain a server result, the microcircuit card executing a second set of instructions applying a chain of operations to the message to obtain a resultant message, comparing the resultant message to the server result, and the server and card mutually authenticating when the server result and resultant message are identical (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly choosing a group of operations that include some combination of operations of first and second chains of operations in either a complemented or uncomplemented state.

Chow discloses a tamper-proof encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9).

However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claim 37, Chow further discloses selecting between using the message in uncomplemented or complemented form (Chow, column 18, lines 50-64, where inputs are complemented or not).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2492